COMISSÃO DAS COMUNIDADES EUROPEIAS

Bruxelas, 17.11.2005
COM(2005) 576 final

LIVRO VERDE

RELATIVO A UM PROGRAMA EUROPEU DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS

(apresentado pela Comissão)

LIVRO VERDE

RELATIVO A UM PROGRAMA EUROPEU DE PROTECÇÃO DAS INFRA-ESTRUTURAS CRÍTICAS

1. CONTEXTO

As infra-estruturas críticas (IC) podem ser danificadas, destruídas ou perturbadas por actos deliberados de terrorismo, catástrofes naturais, negligência, acidentes, actos de pirataria informática, actividades criminosas e comportamentos mal intencionados. Para salvaguardar a vida e os bens das pessoas da UE que podem ser vítimas de terrorismo, catástrofes naturais e acidentes, quaisquer falhas ou manipulações de IC devem, tanto quanto possível, ser breves, infrequentes, geríveis, geograficamente isoladas e pouco lesivas do bem-estar dos Estados-Membros, dos seus cidadãos e da União Europeia. Os recentes ataques terroristas de Madrid e Londres realçaram o risco deste tipo de ataques contra infra-estruturas europeias. A resposta da UE deve ser rápida, coordenada e eficaz.

O Conselho Europeu de Junho de 2004 solicitou à Comissão que elaborasse uma estratégia global de protecção das infra-estruturas críticas. Nessa perspectiva, a Comissão adoptou, em 20 de Outubro de 2004, a Comunicação intitulada "Protecção das infra-estruturas críticas no âmbito da luta contra o terrorismo" em que apresenta sugestões claras sobre como reforçar a prevenção, estado de preparação e capacidade de resposta europeias relativamente a ataques terroristas que afectem infra-estruturas críticas.

As conclusões do Conselho em matéria de "Prevenção, Estado de Preparação e Capacidade de Resposta a Ataques Terroristas" e o "Programa de solidariedade da União Europeia face às consequências das ameaças e dos atentados terroristas", adoptados pelo Conselho em Dezembro de 2004, apoiaram a intenção da Comissão de propor um programa europeu de protecção das infra-estruturas críticas (PEPIC) e aprovaram a criação pela Comissão de uma Rede de Alerta para as Infra-estruturas Críticas (RAIC).

A Comissão organizou dois seminários e apelou à apresentação de ideias e observações por parte dos Estados-Membros. O 1.º Seminário de Protecção das Infra-Estruturas Críticas da UE realizou-se em 6 – 7 de Junho de 2005 com a participação dos Estados-Membros. Na sequência desse seminário, os Estados-Membros apresentaram à Comissão documentação pertinente relativa à abordagem da protecção das infra-estruturas críticas (PIC), bem como observações sobre as ideias debatidas durante o seminário. Estes documentos foram recebidos em Junho e Julho e constituíram a base do aprofundamento da protecção das infra-estruturas críticas. O 2.º seminário de protecção das infra-estruturas críticas da UE decorreu em 12 – 13 de Setembro e destinou-se a promover o debate sobre questões de protecção das infra-estruturas críticas. Participaram neste seminário quer Estados-Membros quer associações industriais. No seu seguimento, a Comissão decidiu apresentar o presente Livro Verde que descreve as opções em relação ao Programa Europeu de Protecção das Infra-estruturas Críticas.

2. OBJECTIVO DO LIVRO VERDE

O Livro Verde destina-se sobretudo a obter reacções sobre eventuais opções estratégicas do PEPIC que contem com a participação de um vasto leque de interessados. A protecção efectiva das infra-estruturas críticas requer comunicação, coordenação e cooperação a nível nacional e da UE entre todas as partes interessadas – os proprietários e os operadores das infra-estruturas, os legisladores, os organismos profissionais e as associações industriais, em cooperação com todos os níveis administrativos, bem como o público em geral.

O Livro Verde apresenta opções sobre a forma como a Comissão pode corresponder ao pedido do Conselho no sentido de estabelecer um PEPIC e uma RAIC e constitui a segunda fase de um processo de consulta relativo ao estabelecimento de um Programa Europeu de Protecção das Infra-estruturas Críticas. Através da apresentação deste Livro Verde, a Comissão espera receber reacções concretas em relação às opções estratégicas expostas no presente documento. Em função dos resultados do processo de consulta, poderá ser apresentado em 2006 um pacote estratégico PEPIC.

3. OBJECTIVOS E ÂMBITO DO PEPIC

3.1. Objectivo global do PEPIC

O objectivo do PEPIC consiste em assegurar a existência de níveis de protecção adequados e uniformes das infra-estruturas críticas, em reduzir ao mínimo as falhas e em facultar meios de recuperação rápida já testados em toda a União Europeia. O nível de protecção pode não ser uniforme em relação a todas as infra-estruturas críticas e depender do impacto causado pelas suas falhas. O PEPIC será um processo permanente, sendo necessária a sua revisão periódica para atender a novas questões e preocupações.

O PEPIC deveria igualmente minimizar tanto quanto possível qualquer impacto negativo que o aumento dos investimentos na segurança possa ter na competitividade de uma dada indústria. Ao calcular a proporcionalidade dos custos, é preciso não esquecer a necessidade de assegurar a estabilidade dos mercados, que é crucial para os investimentos a longo prazo, bem como a influência que a segurança tem na evolução dos mercados de acções e na esfera macroeconómica.

Pergunta

Será este um objectivo adequado do PEPIC? Caso contrário, qual devia ser o objectivo?

3.2. Protecção que o PEPIC devia assegurar

Embora as medidas de gestão das consequências seja idênticas ou análogas no que respeita à maior parte das perturbações, as medidas de protecção podem variar consoante a natureza da ameaça. Os ataques intencionais e as catástrofes naturais são exemplos de ameaças susceptíveis de diminuir significativamente as capacidades de satisfação das necessidades essenciais e de segurança da população, de manutenção da ordem e de prestação de serviços públicos mínimos essenciais, ou de viabilização do funcionamento adequado da economia.

As opções são as seguintes:

a) **Abordagem exaustiva de todos os riscos**: trata-se de uma abordagem global que atenda a riscos quer de ataques intencionais quer de catástrofes naturais, que asseguraria que as sinergias entre as medidas de protecção fossem aproveitadas ao máximo, sem atribuir qualquer ênfase específica ao terrorismo;

b) **Abordagem de todos os riscos com prioridade para o terrorismo:** tratar-se-ia de uma abordagem flexível para assegurar a articulação com outros tipos de riscos, como a ameaça de ataques intencionais e catástrofes naturais, que desse no entanto prioridade ao terrorismo. Se as medidas de protecção de um dado sector industrial fossem consideradas adequadas, as partes interessadas poderiam centrar a sua atenção nas ameaças em relação às quais fossem ainda vulneráveis.

c) **Abordagem em relação aos riscos de terrorismo**: tratar-se-ia de uma abordagem centrada no terrorismo que não prestaria qualquer atenção específica a ameaças mais comuns.

Pergunta

Que abordagem devia adoptar o PEPIC? Porquê?

4. PRINCÍPIOS ESSENCIAIS PROPOSTOS

Sugere-se que os princípios essenciais que se seguem constituam a base do PEPIC:

- **Subsidiariedade**: a subsidiariedade está no cerne do PEPIC, sendo a protecção das infra-estruturas críticas a primeira responsabilidade nacional. Esta responsabilidade incumbirá aos Estados-Membros e aos proprietários/operadores, que agem no âmbito de um enquadramento comum. Por seu turno, a Comissão centrar-se-ia em aspectos ligados à protecção de infra-estruturas críticas com efeitos transfronteiras a nível da UE. Não deve ser afectada a responsabilidade de os proprietários e operadores tomarem as suas próprias decisões e elaborarem planos de protecção dos seus próprios bens.

- **Complementaridade**: o enquadramento comum do PEPIC será complementar em relação às medidas existentes. Nos casos em que existam já mecanismos comunitários, estes devem continuar a ser usados e contribuirão para assegurar a execução global do PEPIC.

- **Confidencialidade**: o intercâmbio de informações sobre a protecção de infra-estruturas críticas decorrerá num contexto de confiança e confidencialidade. Trata-se de uma necessidade, na medida em que factos específicos sobre uma dada infra-estrutura crítica podem ser utilizados para causar falhas ou consequências inaceitáveis em instalações de infra-estruturas críticas. A nível quer da UE quer dos Estados-Membros, as informações sobre instalações críticas serão classificadas e o acesso condicionado numa base de necessidade de conhecimento.

- **Cooperação dos interessados**: todos os interessados, incluindo os Estados-Membros, a Comissão, as associações industriais/empresariais, os organismos de normalização e os proprietários, operadores e utilizadores (definindo-se como "utilizadores" as organizações que exploram e operam a infra-estrutura para fins comerciais ou para a prestação de serviços) têm um papel a desempenhar na protecção das infra-estruturas críticas. Todas as

partes interessadas devem cooperar e contribuir para o desenvolvimento e execução do PEPIC de acordo com os seus papéis e responsabilidades específicos. As autoridades dos Estados-Membros assegurarão a liderança e a coordenação do desenvolvimento e execução de uma abordagem nacional coerente de protecção de infra-estruturas críticas situadas nas respectivas esferas de competência. Os proprietários, operadores e utilizadores serão envolvidos activamente a nível quer nacional quer da UE. Caso não existam normas sectoriais ou não tenham sido ainda estabelecidas normas internacionais, as organizações de normalização podem, se adequado, adoptar normas comuns.

- **Proporcionalidade**: as estratégias e medidas de protecção serão proporcionais ao grau de risco em causa, uma vez que nem todas as infra-estruturas podem ser protegidas em relação a todas as ameaças (por exemplo, as redes de transporte de electricidade são demasiado vastas para que possam ser isoladas ou guardadas). Através da aplicação de técnicas adequadas de gestão do risco, a atenção vai centrar-se nos factores de maior risco, tendo em conta a ameaça, a criticalidade relativa, a relação custo/benefício, o nível de segurança protectora e a eficácia das estratégias de a atenuação existentes.

Pergunta

Estes princípios essenciais são aceitáveis? Alguns são supérfluos? Haverá outros princípios que devam ser considerados?

Concorda que as medidas de protecção devem ser proporcionais ao grau de risco em causa, uma vez que nem todas as infra-estruturas podem ser protegidas em relação a todas as ameaças?

5. UM ENQUADRAMENTO COMUM PARA O PEPIC

A danificação ou perda de uma infra-estrutura num Estado-Membro pode ter consequências negativas em vários outros, bem como na economia europeia em geral. Esta situação torna-se cada vez mais provável na medida em que novas tecnologias (como a Internet) e a liberalização do mercado (como o do abastecimento de gás e electricidade) conduzem a que uma grande parte das infra-estruturas se integre numa rede ainda mais vasta. Neste contexto, as medidas de protecção valem tanto como o seu elo mais fraco, o que significa que pode ser necessário um nível comum de protecção.

A protecção efectiva requer comunicação, coordenação e cooperação a nível nacional, da UE (se for caso disso) e internacional entre todas as partes interessadas. Pode ser criado um enquadramento comum a nível da UE para a protecção de infra-estruturas críticas europeias a fim de assegurar que cada Estado-Membro garante níveis adequados e uniformes de protecção das suas infra-estruturas críticas e evitar a distorção das regras de concorrência no mercado interno. Para apoiar as actividades dos Estados-Membros, a Comissão facilitará a identificação, intercâmbio e divulgação de boas práticas em matéria de PIC ao proporcionar um enquadramento comum da protecção de infra-estruturas críticas. É necessário analisar o âmbito deste enquadramento geral.

O enquadramento comum para o PEPIC deve envolver medidas horizontais que definam a competência e as responsabilidades de todas as partes interessadas na protecção das infra-estruturas críticas e lançar as bases de abordagens sectoriais específicas. Destina-se a complementar medidas sectoriais já existentes a nível comunitário e nos Estados-Membros

por forma a assegurar o máximo nível possível de segurança das infra-estruturas críticas na União Europeia. Deve ser considerado prioritário o trabalho que conduza a um acordo em relação a uma lista comum de definições e sectores de IC.

Uma vez que os vários sectores que envolvem infra-estruturas críticas são muito díspares, será difícil estabelecer de forma exacta quais os critérios a utilizar para identificar e proteger todos eles no âmbito de um enquadramento horizontal; este trabalho deve ser efectuado a nível sectorial. No entanto, é necessário chegar a um entendimento sobre determinadas questões multissectoriais.

Sugere-se portanto o reforço das IC na UE através do estabelecimento de um enquadramento comum para o PEPIC (objectivos e metodologias comuns, por exemplo para estabelecer comparações e interdependências), do intercâmbio de boas práticas e da observância de mecanismos de controlo. O enquadramento comum poderá abranger os seguintes elementos:

- princípios comuns de PIC;
- códigos/normas comummente acordados;
- definições comuns com base nas quais se possa chegar a acordo sobre definições sectoriais específicas (o Anexo 1 inclui uma lista indicativa de definições);
- uma lista comum dos sectores das IC (o Anexo 2 inclui uma lista indicativa de sectores);
- áreas prioritárias em matéria de PIC;
- descrição das responsabilidades das partes interessadas;
- parâmetros estabelecidos de comum acordo;
- metodologias para comparar e atribuir prioridade às infra-estruturas dos diferentes sectores.

Este enquadramento comum minimizará igualmente os possíveis efeitos de distorção da concorrência no mercado interno.

O enquadramento comum para o PEPIC pode ser total ou parcialmente facultativo ou obrigatório, consoante a questão em causa. Ambos os tipos de enquadramento podem complementar medidas sectoriais e horizontais existentes a nível comunitário e dos Estados-Membros; no entanto, só um enquadramento jurídico pode criar uma base jurídica sólida e viável com vista à aplicação coerente e uniforme de medidas de protecção de ICE e permitirá definir claramente as responsabilidades respectivas dos Estados-Membros e da Comissão. Medidas facultativas não vinculativas, muito embora flexíveis, não definem claramente quem faz o quê.

Em função dos resultados de uma análise cuidadosa que atenda devidamente à proporcionalidade das medidas propostas, a Comissão pode recorrer a vários instrumentos, incluindo os legislativos, na sua proposta de PEPIC. Se for caso disso, as propostas de medidas específicas serão acompanhadas de avaliações de impacto.

Perguntas:

Um enquadramento comum pode ser eficaz no reforço da PIC?

Se for necessário um enquadramento legislativo, quais devem ser os seus elementos?

Concorda que os critérios de identificação de vários tipos de ICE e que as medidas de protecção consideradas necessárias devem ser estabelecidas numa base sectorial?

Um enquadramento comum pode contribuir para clarificar as responsabilidades das partes interessadas?

Em que medida deve tal enquadramento comum ser obrigatório ou facultativo?

Qual deve ser o âmbito do enquadramento comum?

Concorda com a lista de termos e definições indicativos constante do Anexo I com base na qual podem ser elaboradas definições sectoriais específicas (se for caso disso)?

Concorda com a lista indicativa de sectores de IC constante do Anexo II?

6. INFRA-ESTRUTURAS CRÍTICAS EUROPEIAS (ICE)

6.1. Definição de infra-estrutura crítica europeia

A definição do que constitui uma infra-estrutura crítica europeia será determinada pelo seu efeito transfronteiras, que indica se o incidente pode ter consequências graves fora do território do Estado-Membro em que a instalação está localizada. Outro elemento a ter em linha de conta é o facto de os regimes de cooperação bilateral em matéria de PIC entre os Estados-Membros constituírem um meio comprovado e eficaz de abordar as IC em ambos os lados das fronteiras entre dois Estados-Membros. Esta cooperação pode complementar o PEPIC.

As ICE podem incluir recursos físicos, serviços, dispositivos de tecnologias da informação, redes e componentes de infra-estruturas que, caso sejam danificados ou destruídos, podem ter consequências graves para a saúde, segurança e bem-estar económico ou social de:

a) dois ou mais Estados-Membros – **inclui certas IC bilaterais (quando relevante)**;

b) três ou mais Estados-Membros – **exclui todas as IC bilaterais**.

Ao analisar o mérito destas opções, é importante atender aos seguintes aspectos:

– o facto de um componente de uma infra-estrutura ser designada como ICE não significa necessariamente que careça de medidas de protecção adicionais. As medidas de protecção existentes, que podem incluir acordos bilaterais entre Estados-Membros, podem ser perfeitamente adequadas e não ser, portanto, alteradas devido à designação de ICE;

– a opção a) pode envolver um número mais elevado de designações;

– a opção b) pode significar que, no que respeita às infra-estruturas que interessam apenas a dois Estados-Membros, não há que prever qualquer intervenção comunitária, mesmo que o grau de protecção seja considerado inadequado por um desses dois Estados-Membros e que o outro Estado-Membro se recuse a tomar medidas. A opção b) pode igualmente conduzir a uma variedade de acordos ou desacordos bilaterais entre os Estados-Membros. A indústria, que frequentemente opera a nível pan-europeu, pode deparar com um grande leque de acordos diferentes que podem envolver custos adicionais.

Além disso, reconhece-se que devem ser analisadas as IC existentes ou provenientes de fora da UE, embora interligadas ou com efeitos directos potenciais nos Estados-Membros da UE.

Pergunta

As ICE devem ser infra-estruturas com efeitos transfronteiras potencialmente graves em dois ou mais Estados-Membros ou em três ou mais Estados-Membros? Porquê?

6.2. Interdependências

Sugere-se que a identificação progressiva de todas as ICE atenda, designadamente, às interdependências. Os estudos de interdependência contribuirão para avaliar as consequências potenciais de ameaças em relação a IC específicas e, em especial, para identificar os Estados-Membros que serão afectados em caso de incidente grave neste domínio.

Devem ser analisada em profundidade as interdependências em e entre empresas, sectores industriais, territórios geográficos e autoridades dos Estados-Membros, nomeadamente as que envolvam tecnologias da informação e da comunicação (TIC). A Comissão, os Estados-Membros e os proprietários/operadores de infra-estruturas críticas devem cooperar na identificação destas interdependências e, sempre que possível, aplicar estratégias adequadas de redução do risco.

Perguntas

Como é possível atender às interdependências?

Tem conhecimento de metodologias adequadas de análise de interdependências?

A que nível se deve proceder à identificação das interdependências: a nível da UE e/ou dos Estados-Membros?

6.3. Fases de implementação das ICE

A Comissão sugere as seguintes fases de implementação das ICE:

(1) A Comissão, em cooperação com o Estado-Membro, elabora critérios específicos a utilizar para identificar as ICE numa base sectorial;

(2) Identificação e verificação progressivas, numa base sectorial, das ICE pelos Estados-Membros e pela Comissão. A decisão de designar uma dada IC como ICE será tomada a nível europeu[1], devido ao carácter transfronteiriço da infra-estrutura em causa;

(3) Os Estados-Membros e a Comissão analisam as lacunas de segurança existentes das ICE numa base sectorial;

(4) Os Estados-Membros e a Comissão definem sectores/infra-estruturas prioritários de acção, tendo em conta as interdependências;

(5) Se for caso disso, relativamente a cada sector, a Comissão e as principais partes interessadas dos Estados-Membros chegam a acordo sobre propostas de medidas mínimas de protecção, que podem incluir normas;

[1] Excepto no que respeita às infra-estruturas ligadas à defesa.

(6) Após a adopção das propostas pelo Conselho, estas medidas são então executadas;

(7) Os Estados-Membros e a Comissão asseguram um controlo periódico. Sempre que necessário, serão efectuadas revisões (medidas e identificação de IC).

Perguntas

É aceitável a lista das fases de implementação das ICE?

Como sugere que a Comissão e os Estados-Membros designem conjuntamente as ICE, dispondo os Estados-Membros de competências e a Comissão de uma visão geral dos interesses europeus? Deve tratar-se de uma decisão de natureza legal?

É necessário um mecanismo de arbitragem se um dado Estado-Membro não aceitar designar como ICE uma infra-estrutura da sua competência?

É necessário verificar as designações? Quem deve ser responsável?

Os Estados-Membros devem poder designar infra-estruturas de outros Estados-Membros ou de países terceiros como infra-estruturas críticas do seu ponto de vista? O que deve suceder se um Estado-Membro, um país terceiro ou uma indústria considerar crítico para si um componente de infra-estrutura de um Estado-Membro?

O que deve suceder se um Estado-Membro a não identificar? É necessário um mecanismo de recurso? Em caso afirmativo, qual?

Um operador deve poder introduzir um recurso se não concordar com a sua designação ou não designação? Em caso afirmativo, junto de quem?

Que metodologias necessitam de ser desenvolvidas para estabelecer sectores/infra-estruturas prioritários de acção? Existem já metodologias adequadas que podem ser adaptadas ao âmbito europeu?

De que forma pode a Comissão participar na análise das lacunas de segurança das ICE?

7. INFRA-ESTRUTURAS CRÍTICAS NACIONAIS (ICN)

7.1. Papel das ICN no PEPIC

Muitas empresas europeias operam em vários países e estão, portanto, sujeitas a obrigações diferentes no que respeita às ICN. Sugere-se, portanto, no interesse dos Estados-Membros e de toda a UE, que cada Estado-Membro proteja as suas ICN no âmbito de um enquadramento comum, a fim de evitar que os proprietários e os operadores de toda a Europa estejam sujeitos a uma grande variedade de enquadramentos que impliquem múltiplas metodologias e a custos adicionais. Para esse efeito, a Comissão sugere que o PEPIC - embora incida sobretudo nas infra-estruturas críticas da UE – não exclua totalmente as infra-estruturas críticas nacionais. No entanto, podem ser ponderadas três opções:

a) Integração total das ICN no PEPIC

b) ICN fora do âmbito do PEPIC

c) Os Estados-Membros podem optar por integrar uma parte das ICN no PEPIC, embora não sejam obrigados a fazê-lo.

Perguntas

A protecção eficaz das infra-estruturas críticas na União Europeia pode requerer a identificação quer das ICE quer das ICN. Concorda que, embora o PEPIC deva centrar-se nas ICE, as ICN não podem ficar totalmente excluídas?

Qual destas opções considera mais adequada para o PEPIC?

7.2. Programas nacionais de PIC

Com base num enquadramento PEPIC comum, os Estados-Membros podem desenvolver programas nacionais de PIC em relação às suas ICN. Os Estados-Membros podem aplicar medidas mais estritas do que as previstas no PEPIC.

Pergunta

É desejável que cada Estado-Membro adopte um programa nacional de PIC com base no PEPIC?

7.3. Organismo de controlo único

Por uma questão de eficácia e coerência, é necessária a designação por cada Estado-Membro de um único o organismo de controlo responsável pela execução global do PEPIC. Podem ser encaradas duas opções:

a) Um só organismo de controlo em matéria de PIC;

b) Um ponto de contacto nacional sem autoridade, incumbindo aos Estados-Membros organizarem-se eles próprios.

Esse organismo pode coordenar, controlar e fiscalizar a execução do PEPIC no seu território e constituir o principal ponto de contacto institucional em matéria de PIC com a Comissão, os restantes Estados-Membros e os proprietários e operadores de PIC. Este organismo pode constituir a base de uma representação nacional em grupos de peritos em matéria de PIC e estar ligado à rede de alerta para as infra-estruturas críticas da União Europeia (RAIC). O Organismo de Coordenação da PIC Nacionais (OCIN) pode coordenar as questões nacionais em matéria de PIC, independentemente da existência de outros organismos ou entidades num Estado-Membro que possam estar já envolvidos em questões de PIC.

A identificação progressiva das ICN pode ser alcançada através da obrigatoriedade para os proprietários e operadores de infra-estruturas de notificar o OCIN de quaisquer actividades empresariais relevantes ligadas à PIC.

O OCIN pode ser responsável pela decisão de designação de uma infra-estrutura sob a sua alçada como ICN. Esta informação fica à disposição exclusiva do Estado-Membro em causa.

As competências específicas podem abranger:

a) A coordenação, controlo e supervisão da aplicação global do PEPIC num Estado-Membro;

b) A função de principal ponto de contacto institucional em questões de PIC com:

   i. a Comissão;

   ii outros Estados-Membros;

   iii. proprietários e operadores de PIC;

c) A participação na designação de infra-estruturas críticas europeias (ICE);

d) A adopção da decisão de designar uma infra-estrutura sob a sua jurisdição como infra-estrutura crítica nacional;

e) A função de autoridade de recurso no que respeita aos proprietários/operadores que não concordem que as suas infra-estruturas sejam designadas como "infra-estruturas críticas";

f) A participação na elaboração de um programa de protecção das infra-estruturas críticas nacionais e nos programas sectoriais específicos de PIC;

g) A identificação das interdependências entre sectores específicos de IC;

h) A contribuição para abordagens sectoriais específicas em relação à PIC através da participação em grupos de peritos. Os representantes dos proprietários e dos cooperadores podem ser convidados a participar no debate. Podem realizar-se reuniões periódicas;

i) A supervisão do processo de elaboração de planos de emergência em relação às IC.

Perguntas

Concorda que apenas os Estados-Membros sejam responsáveis pela designação e gestão de ICN no âmbito de um enquadramento comum do PEPIC?

Considera desejável a designação de um organismo de coordenação da PIC em cada Estado-Membro, globalmente responsável pela coordenação das medidas ligadas à PIC e que respeite simultaneamente as responsabilidades sectoriais existentes (autoridades da aviação civil, Directiva Seveso, etc.)?

Serão adequadas as competências sugeridas para um tal organismo de coordenação? Serão necessárias outras competências?

7.4. Fases de implementação das ICN

A Comissão sugere as seguintes fases de implementação das ICN:

(1) Os Estados-Membros elaboram os critérios específicos a utilizar para identificar as ICN através do recurso ao PEPIC;

(2) Identificação e verificação progressivas, numa base sectorial, das ICN pelos Estados-Membros;

(3) Os Estados-Membros analisam as lacunas de segurança existentes das ICN numa base sectorial;

(4) Os Estados-Membros estabelecem sectores prioritários de acção, tendo em conta, se for caso disso, as interdependências e as prioridades acordadas a nível da UE;

(5) Se pertinente, os Estados-Membros acordam medidas mínimas de protecção em cada sector;

(6) Os Estados-Membros são responsáveis por assegurar que os proprietários/operadores sob a sua jurisdição executem as medidas de implementação necessárias;

(7) Os Estados-Membros asseguram o controlo periódico. Sempre que necessário serão efectuadas revisões (medidas e identificação de IC).

Pergunta

Considera aceitável a lista das fases de implementação das ICN? Há fases supérfluas? Há fases que devam ser aditadas?

8. PAPEL DOS PROPRIETÁRIOS, OPERADORES E UTILIZADORES DAS IC

8.1. Responsabilidades dos proprietários, operadores e utilizadores das IC

A designação de uma IC sugere determinadas responsabilidades dos proprietários e operadores. Podem ser encaradas quatro responsabilidades no que respeita aos proprietários e operadores designados como ICN e ICE:

(1) **Notificação ao organismo pertinente de PIC do Estado-Membro em causa do facto de uma infra-estrutura poder ter um carácter crítico;**

(2) **Designação de um representante de alto nível para agir como funcionário de ligação de segurança (FLS) entre o proprietário/operador e a autoridade PIC competente do Estado-Membro.** O FLS deve participar na elaboração de planos de segurança e de emergência e deve ser o principal funcionário de ligação com o sector de PIC em causa no Estado-Membro e, se for caso disso, com as autoridades responsáveis pela aplicação da lei;

(3) **Elaboração, execução e actualização de um plano de segurança dos operadores (PSO).** Do Anexo 3 consta uma proposta de modelo de PSO.

(4) **Participação,** mediante pedido, **no desenvolvimento de um plano de emergência** em relação às IC, em colaboração com as autoridades dos Estados-Membros competentes em matéria de protecção civil e aplicação da lei.

O PSO pode ser sujeito à aprovação da autoridade sectorial competente do Estado-Membro em matéria de PIC no âmbito da supervisão global do OCIN, independentemente de se tratar de uma ICN ou de uma ICE que garanta a coerência das medidas de segurança tomadas por proprietários e operadores específicos e, em termos gerais, pelos sectores em causa. Em contrapartida, os proprietários e operadores podem receber informações e apoio em relação a ameaças pertinentes, ao desenvolvimento de boas práticas e, se adequado, apoio na avaliação de interdependências e vulnerabilidades através do OCIN e, se for caso disso, da Comissão.

Os Estados-Membros podem estabelecer um prazo para a elaboração de PSO pelos proprietários e operadores de ICN e ICE (neste último caso, a Comissão participará igualmente) e podem estabelecer coimas em relação a situações em que estes prazos não sejam respeitados.

Sugere-se que o plano de segurança dos operadores (PSO) identifique as infra-estruturas críticas do proprietário/operador e estabeleça soluções de segurança pertinentes com vista à sua protecção. O PSO deve descrever os métodos e o procedimento a adoptar para observar o PEPIC, os programas nacionais de PIC e os programas sectoriais específicos pertinentes de PIC. O PSO pode constituir um meio para uma abordagem da base para o topo na regulamentação da PIC que dê mais peso (e também mais responsabilidade) ao sector privado.

Em casos específicos, no caso de determinadas infra-estruturas, como redes eléctricas e de informação, será irrealista (em termos práticos e financeiros) esperar que os proprietários e operadores garantam níveis idênticos de segurança de todos os seus bens. Nesses casos, sugere-se que os proprietários e operadores possam, em colaboração com as autoridades competentes, identificar os pontos críticos (nós) de uma rede física ou de informação em que possam ser centradas as medidas de protecção da segurança.

O PSO pode incluir medidas de segurança organizadas em torno de duas vertentes:

- **Medidas de segurança permanentes**, que identificarão investimentos e meios de segurança imprescindíveis que não possam ser instalados pelo proprietário/operador a curto prazo. O proprietário/operador pode manter um estado de alerta permanente em relação a ameaças potenciais que não deve perturbar as suas actividades económicas, administrativas e sociais regulares.

- **Medidas de segurança progressivas**, que podem ser activadas consoante o grau de ameaça. O PSO deve, portanto, prever vários regimes de segurança adequados aos vários graus de ameaça existentes no Estado-Membro em que as infra-estruturas estão situadas.

Propõe-se que o incumprimento por parte de um proprietário ou operador de IC da obrigação de elaborar um PSO, de contribuir para o desenvolvimento de planos emergência e de designar um FLS possa conduzir a uma sanção financeira.

Perguntas

Há responsabilidades potenciais dos proprietários/operadores de infra-estruturas críticas aceitáveis em termos de aumento da segurança das infra-estruturas críticas? Qual será o seu custo provável?

Devem os proprietários e operadores ser obrigados a comunicar que as suas infra-estruturas podem ter um carácter crítico? Considera útil o conceito de PSO? Porquê?

As obrigações propostas são proporcionais aos custos em causa?

Que direitos podem ser atribuídos pelas autoridades dos Estados-Membros e pela Comissão aos proprietários e operadores de infra-estruturas críticas?

8.2. Diálogo com os proprietários, operadores e utilizadores das IC

O PEPIC poder implicar os proprietários e operadores em parcerias. O êxito de qualquer programa de protecção depende da cooperação e do grau de participação dos proprietários e operadores. A nível dos Estados-Membros, os proprietários e operadores de PIC podem ser estreitamente associados à evolução da PIC através de contactos periódicos com o OCIN.

A nível da UE podem ser criados fóruns para facilitar o intercâmbio de opiniões sobre questões gerais e sectoriais específicas em matéria de PIC. Uma abordagem comum em relação à participação do sector privado em questões ligadas à PIC que congregue todas as partes interessadas do domínio público e privado proporcionará aos Estados-Membros, à Comissão e à indústria uma plataforma importante de comunicação sobre questões que possam surgir em matéria de PIC. Os proprietários, operadores e utilizadores de IC podem contribuir para o desenvolvimento de orientações comuns, normas em matéria de boas práticas e, se for caso disso, intercâmbio de informação. Este diálogo contribuirá para moldar revisões futuras do PEPIC.

Se pertinente, a Comissão pode incentivar a criação de associações de indústrias/empresas ligadas à PIC a nível da UE. Os dois objectivos fundamentais são a manutenção da competitividade da indústria europeia e a melhoria da segurança dos cidadãos da UE.

Pergunta

Como deve ser estruturado o diálogo com os proprietários, operadores e utilizadores de IC?

Quem deve representar os proprietários, operadores e utilizadores no diálogo público-privado?

9. MEDIDAS DE APOIO AO PEPIC

9.1. Rede de alerta para as infra-estruturas críticas da União Europeia (RAIC)

A Comissão elaborou vários sistemas de alerta rápido que possibilitam uma resposta concreta, coordenada e eficaz em caso de emergências, incluindo de origem terrorista. Em 20 de Outubro de 2004, a Comissão anunciou a criação de uma rede centralizada que assegura o intercâmbio rápido de informação entre todos os sistemas de alerta rápido da Comissão e os serviços da Comissão em causa (ARGUS).

A Comissão sugere a criação de uma RAIC que possa fomentar o desenvolvimento de medidas de protecção adequadas através do intercâmbio de boas práticas de forma segura e constituir um veículo de informação sobre ameaças e alertas imediatos. O sistema assegurará que as pessoas certas tenham acesso à informação adequada na altura exacta.

São possíveis três opções no que respeita ao desenvolvimento de uma RAIC:

(1) **A RAIC pode ser um fórum limitado ao intercâmbio de ideias e de boas práticas em matéria de PIC** destinado a apoiar os proprietários e operadores de IC. Este fórum pode ser constituído por uma rede de peritos e uma plataforma electrónica de intercâmbio de informações pertinentes num ambiente seguro. A Comissão desempenhará um papel importante na recolha e divulgação destas informações. Esta opção não proporcionará os alertas rápidos necessários sobre ameaças iminentes. No entanto, o seu âmbito pode ser alargado futuramente.

(2) **A RAIC deve ser um sistema de alerta rápido (SAR) entre os Estados-Membros e a Comissão.** Esta opção aumenta a segurança das infra-estruturas críticas ao proporcionar informações limitadas a ameaças e alertas imediatos. O objectivo é facilitar o intercâmbio rápido de informações sobre ameaças potenciais entre proprietários e operadores de IC. O SAR não envolverá a partilha de informações a longo prazo. Destina-se ao intercâmbio rápido de informações sobre ameaças iminentes a infra-estruturas específicas.

(3) **A RAIC deve ser um sistema de comunicação/alerta a vários níveis com duas funções distintas:** a) um sistema de alerta rápido (SAR) entre os Estados-Membros e a Comissão e b) um fórum de intercâmbio de ideias e de boas práticas em matéria de PIC destinado a apoiar os proprietários e operadores de IC, composto por uma rede de peritos e uma plataforma electrónica de intercâmbio de dados.

Independentemente da opção seleccionada, a RAIC complementará as redes existentes, devendo ser evitadas duplicações. A longo prazo, a RAIC pode ser ligada a todos os proprietários e operadores pertinentes de cada Estado-Membro, por exemplo através do OCIN. Os alertas e as boas práticas podem ser canalizados através deste organismo, que deveria ser o único serviço directamente ligado à Comissão e, por conseguinte, a todos os restantes Estados-Membros. Os Estados-Membros podem utilizar os respectivos sistemas de informação existentes para a criação das suas infra-estruturas nacionais RAIC de ligação entre as autoridades e proprietários e operadores específicos. Importa frisar que estas redes nacionais podem ser utilizadas pelos organismos competentes de PIC dos Estados-Membros e pelos proprietários e operadores como sistema de comunicação bidireccional.

Será lançado um estudo para determinar o âmbito e as especificações técnicas necessárias para a futura interface RAIC com os Estados-Membros.

Perguntas

Qual deve ser a estrutura da rede RAIC para promover os objectivos do PEPIC?

Os proprietários e operadores de IC devem estar ligados à RAIC?

9.2. Metodologias comuns

Os Estados-Membros dispõem de níveis de alerta diferentes que correspondem a situações igualmente diferentes. Actualmente, não é possível determinar se, por exemplo, um nível elevado num Estado-Membro equivale ao nível elevado de outro Estado-Membro. Tal facto pode conduzir a dificuldades na definição de prioridades pelas empresas transnacionais em matéria de despesas em medidas de protecção. Pode, portanto, ser oportuno procurar harmonizar ou aferir os vários níveis.

A cada nível de ameaça pode corresponder um nível de preparação que desencadeie em termos genéricos medidas de segurança comuns e, se adequado, o recurso a medidas de segurança específicas. Os Estados-Membros que não pretendam aplicar uma dada medida podem fazer face a uma ameaça específica através de medidas de segurança alternativas.

Pode ser ponderada uma metodologia comum de identificação e classificação de ameaças, capacidades, riscos e vulnerabilidades que permita chegar a conclusões sobre a possibilidade, probabilidade e grau de gravidade da ameaça em termos de perturbação da infra-estrutura. Tal facto envolverá a classificação e prioritização do risco, em que os riscos poderia ser definidos em termos da respectiva probabilidade de ocorrência, impacto e relação com outras áreas ou processos de risco.

Perguntas

Em que medida é desejável e exequível harmonizar ou aferir níveis de alerta diferentes?

Deve ser ponderada uma metodologia comum de identificação e classificação de ameaças, capacidades, riscos e vulnerabilidades que permita chegar a conclusões sobre a possibilidade, probabilidade e grau de gravidade de uma ameaça?

9.3. Financiamento

Na sequência de uma iniciativa do Parlamento Europeu (criação de uma nova rubrica orçamental – projecto-piloto de "Luta contra o terrorismo" – no orçamento de 2005), a Comissão decidiu, em 15 de Setembro, afectar 7 milhões de euros ao financiamento de um conjunto de acções de promoção da prevenção, preparação e resposta em relação a ataques terroristas, incluindo a gestão das consequências, a protecção de infra-estruturas críticas, o financiamento do terrorismo, os explosivos e a radicalização violenta. Mais de dois terços deste orçamento são consagrados à elaboração do futuro programa europeu de protecção de infra-estruturas críticas, à integração e desenvolvimento das capacidades necessárias para a gestão de crises de âmbito transnacional resultantes de possíveis ataques terroristas e a medidas de emergência eventualmente necessárias para enfrentar uma ameaça significativa ou a ocorrência de um tal ataque. Tudo indica que esse financiamento seja mantido em 2006.

Entre 2007 e 2013, o financiamento será assegurado pelo Programa-Quadro de Segurança e Protecção das Liberdades. Este incluirá um programa específico em matéria de "Prevenção, Preparação e Gestão das Consequências do Terrorismo"; a proposta da Comissão afectou um montante de 137,4 milhões de euros para identificar as necessidades e desenvolver normas técnicas comuns de protecção de infra-estruturas críticas.

O programa contemplará o financiamento comunitário de projectos apresentados por autoridades nacionais, regionais e locais com vista à protecção de infra-estruturas críticas. O

programa centra-se na identificação de necessidades de protecção e na prestação de informações com vista ao desenvolvimento de normas comuns e de avaliações de ameaças e riscos a fim de proteger infra-estruturas críticas ou para o desenvolvimento de planos de emergência específicos. A Comissão deve utilizar as competências de que dispõe ou pode contribuir para financiar estudos relativos a interdependências em vários sectores específicos. Incumbe então sobretudo aos Estados-Membros ou aos proprietários e operadores melhorar a segurança das suas infra-estruturas de acordo com as necessidades identificadas. O próprio programa não financia a melhoria da protecção de infra-estruturas críticas. Podem ser utilizados empréstimos de instituições financeiras para a melhoria da segurança de infra-estruturas nos Estados-Membros de acordo com as necessidades identificadas no âmbito do programa, assim como para a aplicação de normas comuns. A Comissão está disposta a apoiar estudos sectoriais para avaliar o impacto financeiro que a melhoria da segurança de infra-estruturas pode ter na indústria.

A Comissão está a financiar projectos de investigação de apoio à protecção de infra-estruturas críticas no âmbito da acção preparatória relativa à investigação em matéria de segurança[2] (2004 – 2006) e tem previstas actividades mais significativas neste domínio na proposta de decisão do Conselho e do Parlamento Europeu relativa ao 7º Programa-Quadro de Investigação da CE (COM(2005)119 final)[3] e na proposta de Decisão do Conselho relativa ao programa específico "Cooperação" para execução do 7º programa-quadro (COM(2005)440 final). A investigação dirigida destinada à criação de estratégias e instrumentos práticos de limitação do risco é extremamente importante para a securização das infra-estruturas críticas da UE a médio e a longo prazo. Toda a investigação em matéria de segurança, designadamente neste domínio, será sujeita a uma análise ética para assegurar a sua compatibilidade com a Carta dos Direitos Fundamentais. A necessidade de investigação tenderá a aumentar à medida que aumente o número de dependências entre infra-estruturas.

Perguntas

Como avalia o custo e o impacto da execução das medidas apresentadas no presente Livro Verde no que respeita à administração pública e à indústria? Considera-as proporcionadas?

9.4. Avaliação e acompanhamento

A avaliação e acompanhamento da execução do PEPIC aponta para um processo a vários níveis que requer a participação de todas as partes interessadas:

- **A nível da UE, pode ser estabelecido um mecanismo de avaliação por pares**, em que os Estado-Membros e a Comissão colaborarão na avaliação do nível global de execução do PEPIC em cada Estado-Membro. A Comissão pode elaborar relatórios intercalares anuais sobre a execução do PEPIC.

---

2 O montante total das dotações nos orçamentos de 2004 e 2005 ascendeu a 30 milhões de euros. Em relação a 2006, a Comissão propôs o montante de 24 milhões de euros, que está a ser analisado pela autoridade orçamental.

3 A proposta de orçamento da Comissão em relação a actividades de investigação ligadas à segurança e ao espaço no âmbito do 7.º programa-quadro de I&D envolve um montante de 570 milhões de euros (COM(2005)119 final).

- **A Comissão apresentaria um relatório intercalar aos Estados-Membros e outras instituições em cada ano de calendário** através de um documento de trabalho elaborado pelos seus serviços.

- **A nível dos Estados-Membros, os respectivos OCIN podem acompanhar a execução global do PEPIC no seu território e assegurar a observância do ou dos programas nacionais de PIC e dos programas sectoriais específicos de PIC**, para garantir que sejam efectivamente executados, através de relatórios anuais ao Conselho e à Comissão.

A execução do PEPIC será um processo dinâmico, em mutação e avaliação constante, para que se possa adaptar a um mundo em evolução e aproveitar os ensinamentos obtidos. As avaliações por pares e os relatórios de acompanhamento dos Estados-Membros podem ser alguns dos instrumentos utilizados para rever o PEPIC e para sugerir novas medidas de melhoria da protecção de infra-estruturas críticas.

Podem ser facultadas à Comissão informações pertinentes dos Estados-Membros relativamente às ICE com vista ao desenvolvimento de avaliações comuns da vulnerabilidade, de planos de gestão das consequências e de normas comuns de protecção de IC, de definição de prioridades das actividades de investigação e, se necessário, de regulamentação e harmonização. Estas informações serão classificadas e estritamente confidenciais.

A Comissão pode acompanhar várias iniciativas dos Estados-Membros, incluindo as que prevêem consequências financeiras para os proprietários e operadores incapazes de restabelecer serviços essenciais aos cidadãos dentro de um prazo máximo definido.

Pergunta

Que tipo de mecanismo de avaliação será necessário para o PEPIC? Será suficiente o mecanismo acima referido?

As respostas devem ser enviadas até 15 de Janeiro de 2006 para o seguinte endereço de correio electrónico: **JLS-EPCIP@cec.eu.int**. Estas respostas serão tratadas confidencialmente a menos que o inquirido declare explicitamente que as pretende tornar públicas, sendo nesse caso publicadas no sítio Internet da Comissão.

ANNEXES

ANNEX 1

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage.

CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service.

Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- Procedures and where relevant individuals that exert control over critical infrastructure functions.
- Objects having cultural or political significance as well as "soft targets" which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS.

The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State's national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.

- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major. Among the criteria which can be used to assess impact are:

  - Public (number of population affected, loss of life, medical illness, serious injury, evacuation);

  - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);

  - Environment (effect on the public and surrounding location);

  - Interdependency (between other critical infrastructure elements).

  - Political effects (confidence in the ability of government);

  - Psychological effects (may escalate otherwise minor events). both during and after the incident and at different spatial levels (e.g. local, regional, national and international)

- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator's critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources.

Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis.

Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

ANNEX 2

INDICATIVE LIST OF CRITICAL INFRASTRUCTURE SECTORS

Sector		Product or service	
I	Energy	1	Oil and gas production, refining, treatment and storage, including pipelines
		2	Electricity generation
		3	Transmission of electricity, gas and oil
		4	Distribution of electricity, gas and oil
II	Information, Communication Technologies, ICT	5	Information system and network protection
		6	Instrumentation automation and control systems (SCADA etc.)
		7	Internet
		8	Provision of fixed telecommunications
		9	Provision of mobile telecommunications
		10	Radio communication and navigation
		11	Satellite communication
		12	Broadcasting
III	Water	13	Provision of drinking water
		14	Control of water quality
		15	Stemming and control of water quantity
IV	Food	16	Provision of food and safeguarding food safety and security
V	Health	17	Medical and hospital care
		18	Medicines, serums, vaccines and pharmaceuticals
		19	Bio-laboratories and bio-agents
VI	Financial	20	Payment services/payment structures (private)
		21	Government financial assignment
VII	Public & Legal Order and Safety	22	Maintaining public & legal order, safety and security
		23	Administration of justice and detention
VIII	Civil administration	24	Government functions
		25	Armed forces
		26	Civil administration services
		27	Emergency services
		28	Postal and courier services
IX	Transport	29	Road transport
		30	Rail transport
		31	Air traffic
		32	Inland waterways transport
		33	Ocean and short-sea shipping
X	Chemical and nuclear industry	34	Production and storage/processing of chemical and nuclear substances
		35	Pipelines of dangerous goods (chemical substances)
XI	Space and Research	36	Space
		37	Research

ANNEX 3

OPERATOR SECURITY PLAN

The possible contents of the OSP should include an introduction and a classified detail part (not accessible outside the relevant MS authorities). The classified part would begin with a presentation of the operator and describe the legal context of its CI activities. The OSP would then go on to presenting the details on the criticality of the infrastructure concerned, taking into consideration the operator's objectives and the Member State's interests. The critical points of the infrastructure would be identified and their security requirements presented. A risk analysis based on major threat scenarios, vulnerability of each critical point, and potential impact would be conducted. Based on this risk analysis, relevant protection measures should be foreseen.

Introduction)

Contains information concerning the pursued objectives and the main organisational and protection principles.

Detailed part *(classified)*

– **Presentation of the operator**

Contains a description of the operator's activities, organization and connections with the public authorities. The details of the operator's Security Liaison Office (SLO) are given.

– **Legal context**

The operator addresses the requirements of the National CIP Programme and the sector specific CIP programme where relevant.

– **Description of the criticality of the infrastructure**

The operator describes in detail the critical services/products he provides and how particular elements of the infrastructure come together to create an end-product. Details should be provided concerning:

- material elements;
- non-material elements (sensors, command, information systems);
- human elements (decision-maker, expert);
- access to information (databases, reference systems);
- dependence on other systems (energy, telecoms);
- specific procedures (organisation, management of malfunctions, etc.).

– **Formalisation of security requirements**

The operator identifies the critical points in the infrastructure, which could not be easily replaced and whose destruction or malfunctioning could significantly disrupt the operation of the activity or seriously endanger the safety of users, customers or employees or result in essential public needs not being satisfied. The security of these critical points is then addressed.

The owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) of critical infrastructure would have to identify the critical points of their infrastructure, which would be deemed restricted areas. Access to restricted areas should be monitored in order to ensure than no unauthorised persons and vehicles enter such areas. Access would only be granted to security cleared personnel. The relevant background security checks (if deemed necessary by a MS CIP sector authority) should be carried out by the Member State in which the critical infrastructure is located.

– **Risk analysis and management**

The operator conducts and risk analysis concerning each critical point.

– **Security measures**

The operator presents the security measures arranged around two headings:

- Permanent security measures, which will identify indispensable security investment and means, which cannot be installed by the owner/operator in a hurry. The owner/operator will maintain a standing alertness against potential threats, which will not disturb its regular economic, administrative and social activities. This heading will include information concerning general measures; technical measures (including installation of detection, access control, protection and prevention means); organizational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems.

- Graduated security measures, which may be activated according to varying threat levels. The OSP will therefore foresee various security regimes adapted to possible threat levels existing in the Member State.

– **Presentation and application**

The operator will prepare detailed information sheets and instructions on how to react to various situations.

– **Monitoring and updating**

The operator sets out the relevant monitoring and updating mechanisms which will be used.